What is claimed is:

1. A method for a capacity planning server in a packet network to calculate				
access router to access router traffic matrixes by using ingress and egress files				
derived from flow records, each ingress file comprising a plurality of ingress				
records in which each ingress record represents an incoming flow, each egress file				
comprising a plurality of egress records in which each egress record represents an				
outgoing flow, the method comprising the steps of:				

identifying ingress and egress records in the ingress and egress files that match; and

calculating a traffic matrix using the matched ingress and egress records.

- 2. The method of claim 1 wherein the step of calculating a traffic matrix further comprises the step of creating a hash set for each egress file.
- 3. The method of claim 2 wherein the step of calculating a traffic matrix further comprises the step of creating a key value by concatenating source addresses and destination addresses from an egress record.
- 4. The method of claim 3 wherein the step of calculating a traffic matrix further comprises the step of adding the key value to the hash set.
- 5. The method of claim 4 wherein the step of calculating a traffic matrix further comprises the step of creating a key value by concatenating source addresses and destination addresses from an ingress record.
- 6. The method of claim 5 wherein the step of calculating a traffic matrix further comprises the step of performing a test to determine if the key value for an ingress record exists in a hash set for an egress file.

- 7. The method of claim 6 wherein the step of calculating a traffic matrix further comprises the step of annotating an ingress record with indexes of egress routers for a flow record.
 - 8. The method of claim 7 wherein the step of calculating a traffic matrix further comprises the step of incrementing an egress router count in the ingress record when the ingress record is annotated.
 - 9. The method of claim 8 wherein the step of calculating a traffic matrix further comprises the step of searching the hash set for every egress file for the key value for every ingress record.
 - 10. The method of claim 9 wherein the step of calculating a traffic matrix further comprises the step of calculating the traffic matrix elements by processing the annotated ingress records.
 - 11. The method of claim 10 wherein the step of calculating a traffic matrix further comprises the step of identifying specific elements in a traffic matrix using data from an annotated ingress record.
 - 12. The method of claim 11 wherein the step of calculating a traffic matrix further comprises the step of identifying specific elements by ingress router index, egress router indexes, and type-of-service.
 - 13. The method of claim 12 wherein the step of calculating a traffic matrix further comprises the step of adding byte and packet counts from an annotated ingress record to the traffic matrix elements.
 - 14. The method of claim 1 wherein the traffic matrices are calculated using non-sampled flow records.

4

matrix.

1	15.	The method of claim 14 wherein the traffic matrices are calculated for a		
2	virtual private network.			
1	16.	The method of claim 1 wherein the traffic matrices are calculated using		
2	sampled flow records.			
1	17.	The method of claim 16 wherein the traffic matrix is calculated for a		
2	virtual private network.			
1	18.	The method of claim 16 further comprising the steps of:		
2		using data from the traffic matrix to compute a distribution matrix;		
3		post-processing the traffic matrix; and		
4		outputting the traffic matrix.		
1	19.	The method of claim 18 wherein the step of post-processing the traffic		
2	matrix further comprises the step of determining the total bytes and packets for			
3	each row of the traffic matrix.			
1	20.	The method of claim 19 wherein the step of post-processing the traffic		
2	matrix further comprises the step of dividing the bytes and packets for each entry			
3	in the	traffic matrix by the totals computed for that row.		
1	21	The weether the falcium 20 replacements the etem of most preceding the traffic		
1	21.	The method of claim 20 wherein the step of post-processing the traffic further comprises the step of determining the unmatched ingress records		
2		ch row of the traffic matrix.		
3	ior ea	ch fow of the traffic matrix.		
1	22.	The method of claim 21 wherein the step of post-processing the traffic		
2		x further comprises the step of assigning the unmatched ingress records to all		
_	***********			

potential egress routers in the same percentages computed for the distribution

23.	A method for a capacity planning server in a packet network to calculate
servic	e node to service node traffic matrixes by using ingress and egress files
derive	ed from flow records, each ingress file comprising a plurality of ingress
record	ls in which each ingress record represents an incoming flow, each egress file
comp	rising a plurality of egress records in which each egress record represents an
outgo	ing flow, the method comprising the steps of:

identifying ingress and egress records in the ingress and egress files that match; and

calculating a traffic matrix using the matched ingress and egress records.

- 24. The method of claim 23 wherein the step of calculating a traffic matrix further comprises the step of creating a hash set for each egress file.
- 25. The method of claim 24 wherein the step of calculating a traffic matrix further comprises the step of creating a key value by concatenating source addresses and destination addresses from an egress record.
- 26. The method of claim 25 wherein the step of calculating a traffic matrix further comprises the step of adding the key value to the hash set.
- 27. The method of claim 26 wherein the step of calculating a traffic matrix further comprises the step of creating a key value by concatenating source addresses and destination addresses from an ingress record.
- 28. The method of claim 27 wherein the step of calculating a traffic matrix further comprises the step of performing a test to determine if the key value for an ingress record exists in a hash set for an egress file.
- 29. The method of claim 28 wherein the step of calculating a traffic matrix further comprises the step of annotating an ingress record with indexes of egress routers for a flow record.

1	30.	The method of claim 29 wherein the step of calculating a traffic matrix
2	further	comprises the step of incrementing an egress router count in the ingress
3	record	when the ingress record is annotated.

- 31. The method of claim 30 wherein the step of calculating a traffic matrix further comprises the step of searching the hash set for every egress file for the key value for every ingress record.
- 32. The method of claim 31 wherein the step of calculating a traffic matrix further comprises the step of calculating the traffic matrix elements by processing the annotated ingress records.
- 33. The method of claim 32 wherein the step of calculating a traffic matrix further comprises the step of identifying specific elements in a traffic matrix using data from an annotated ingress record and a configuration file.
- 34. The method of claim 33 wherein the step of calculating a traffic matrix further comprises the step of mapping an access router name to a service node index.
- 35. The method of claim 34 wherein the step of calculating a traffic matrix further comprises the step of identifying the traffic matrix elements by ingress service node index, egress service node indexes, and type-of-service.
- 36. The method of claim 35 wherein the step of calculating a traffic matrix further comprises the step of adding byte and packet counts from an annotated ingress record to the traffic matrix elements.
- 37. The method of claim 23 wherein the traffic matrices are calculated using non-sampled flow records.

1	38.	The method of claim 37 wherein the traffic matrices are calculated for a		
2	virtual	virtual private network.		
1	39.	The method of claim 23 wherein the traffic matrices are calculated using		
2	sample	sampled flow records.		

- 40. The method of claim 39 wherein the traffic matrix is calculated for a virtual private network.
- 41. The method of claim 39 further comprising the steps of:
 using data from the traffic matrix to compute a distribution matrix;
 post-processing the traffic matrix; and
 outputting the traffic matrix.
- 42. The method of claim 41 wherein the step of post-processing the traffic matrix further comprises the step of determining the total bytes and packets for each row of the traffic matrix.
- 43. The method of claim 42 wherein the step of post-processing the traffic matrix further comprises the step of dividing the bytes and packets for each entry in the traffic matrix by the totals computed for that row.
- 44. The method of claim 43 wherein the step of post-processing the traffic matrix further comprises the step of determining the unmatched ingress records for each row of the traffic matrix.
 - 45. The method of claim 44 wherein the step of post-processing the traffic matrix further comprises the step of assigning the unmatched ingress records to all potential egress routers in the same percentages computed for the distribution matrix.